

09917000 1895227  
531 Rec'd PCT... 912690  
16 AUG 2001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
AS DESIGNATED/ELECTED OFFICE DO/EO/US

U.S. Patent Application No.: Applied For	)	
	)	Group Art Unit: Unknown
International Application No.: PCT/EP99/0998	)	
	)	Examiner: Unknown
International Filing Date: 15 December 1999	)	
	)	Docket No: 13189.138
Priority Date: 16 February 1999	)	
	)	
For: Method And Apparatus For Generating	)	
Data Stream And Method And Apparatu	)	
For Playing A Data Stream	)	
	)	
Applicants (Inventors):	)	
Niels Rump, Juergen Koller and Karlhein	)	
Brandenburg	)	

ATTENTION: EO/US  
BOX PCT  
ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, DC 20231

August 16, 2001

Dear Sir:

**FIRST PRELIMINARY AMENDMENT**

In the Specification:

Please substitute the attached specification entitled "Final version of PCT/EP99/09980 for the prosecution at the USPTO to be filed as first preliminary amendment" for the original PCT specification.

In the Claims:

Please substitute the enclosed claims 1 - 22, on pages 28 - 34, inclusive, attached to the substitute specification, for original claims 1 - 22.

U.S. Patent Application No.: Applied For  
International Application No.: PCT/EP99/09980  
First Preliminary Amendment  
Page 1  
Doc. 1575

In the Abstract:

Please substitute the enclosed abstract, attached to the substitute specification on page 35 for the original abstract.

**REMARKS**

Applicants respectfully request that the Examiner base the examination upon the attached substitute specification, claims, and abstract. An Annotated Copy Of Final Version Of PCT/EP99/09980 is enclosed showing the revisions made in the substitute specification, claims, and abstract.

The PCT specification, claims, and abstract have been revised to conform to U.S. requirements. It is believed that no new matter was introduced in revising the specification, claims, and abstract.

In view of the foregoing amendments, it is believed that the application, including claims 1 – 22 is in condition for allowance, and favorable action is respectfully requested. The Examiner is invited to contact the undersigned by collect telephone call to advance the prosecution in any respect.

No additional fee for this Preliminary Amendment is seen to be required. If any additional fee is required, please charge it to Deposit Account No. 50-1848.

Respectfully submitted,  
**PATTON BOGGS LLP**

By: \_\_\_\_\_

Carl A. Forest, Reg. No. 28,494

Telephone: (303) 379-1114

Facsimile: (303) 379-1155

**Customer No.: 24283**

**U.S. Patent Application No.: Applied For**  
**International Application No.: PCT/EP99/09980**  
**First Preliminary Amendment**

**Page 2**

Doc. 1575

09/913690  
531 Rec'd PCT. 16 AUG 2001

National Phase of PCT/EP99/09980 in U.S.A.

Title: Method and Apparatus for Generating a Data Stream and  
Method and Apparatus for Playing a Data Stream

Applicants: RUMP, Niels et al.

---

Final version of PCT/EP99/09980 for the prosecution at the  
USPTO to be filed as first preliminary amendment

---

5/PRTS

09/913690  
531 Rec'd PCT 16 AUG 2001

5       **Method and Apparatus for Generating a Data Stream and  
Method and Apparatus for Playing a Data Stream**

Field of the Invention

10    The present invention relates to the encryption or decryption of payload data, like e.g. audio and/or video data and especially to audio and/or video data present in the form of a data stream comprising a header and a payload data block.

15

Background of the Invention and Prior Art

20    With the occurrence of telecommunication networks and in particular due to the huge spreading of multimedia data-capable personal computers and, most recently, of so-called solid state players, a need has arisen to market digital multimedia data, such as digital audio data and/or digital video data, commercially. Telecommunication networks for  
25    example can be analog telephone lines, digital telephone lines, such as ISDN, or the Internet. Among the commercial providers of multimedia products there is a need to sell or lend multimedia data, wherein it should be possible for a costumer to be able to select a certain product individually at any time from a certain catalogue, this product  
30    then of course being only allowed to be used by the costumer who has paid for it.

35    Unlike well-known encrypted television programs, such as the television channel Premiere, in which the emitted data is encrypted in the same way for all users who have acquired a suitable decryption device by paying a certain

5 charge, the present invention is to provide methods and devices enabling an individual, customer-selective and safe encryption and decryption of multimedia data. Unlike the television channels mentioned above which give a fixed program all of which the user has to decide for, the methods  
10 and devices of the present invention enable a maximum freedom of selection for the user, which means that the user has only to pay for those products he or she actually wants to use.

15 DE 196 25 635 C1 describes methods and devices for encrypting and decrypting multimedia data, the multimedia data being present in the form of an encrypted multimedia file comprising a destination data block and a payload data block. Parts of the destination data block and at least  
20 some parts of the payload data block are encrypted by means of different keys, especially symmetrical encryption methods being used.

Further, in the method for encrypting or decrypting multimedia data described in DE 196 256 35 C1 a user index is  
25 entered into a determination data block of a bitstream with encrypted multimedia data that identifies the user authorized to use an encrypted multimedia data stream. If this user index identifies merely one person, this method is  
30 only safe against unauthorized copying if that person who has purchased an encrypted multimedia data stream acts correctly and legally. This can, however, not always be guaranteed. If the person who has purchased an encrypted multimedia data stream legally carries out copying, it will not  
35 be possible to see from a copy who has copied it. The origin of the copy can therefore not be tracked down anymore

5 which will open the way for violations of copyrights, incorrect behaviour assumed.

However, if the user index does , not only identify the user as a person but a specific player of a user, like e.g.  
10 the PC of the user, a safety is achieved in such a way that the user can play the encrypted multimedia data stream only on the player identified by the user index regardless whether the user behaves legally or illegally.

15 However, the problem with this solution is the fact that it is not flexible, i.e. it dictates the user where he has to play the purchased multimedia data stream due to the copyright protection. There is not a lot of imagination needed to predict that such system will only find little accep-  
20 tance at the market especially when thinking about the fact that a number of players exist in a normal household. Such players can include for example a personal computer, a laptop, a hifi system, a car hifi system, a video recorder, a solid state player, etc.

25

### Summary of the Invention

Therefore, it is the object of the present invention to  
30 provide a flexible concept for selectively providing multimedia data that on the one hand finds acceptance at the market and at the other hand takes copyright aspects into consideration.

35

In accordance with a first aspect of the present invention, this object is achieved by a method for generating a second

5 data stream from a first data stream which comprises a  
first header and a first payload data block with payload  
data, the method comprising the following steps: extracting  
the first header from the first data stream; generating a  
second header for the second data stream; entering at least  
10 a part of the first header into the second header, the part  
of the first header including information which allows con-  
clusions as to the origin of the payload data; and generat-  
ing a second payload data block having the same payload  
data as the payload data block of the first data stream, so  
15 as to obtain the second data stream.

In accordance with a second aspect of the present inven-  
tion, this object is achieved by a method for playing a se-  
cond data stream which comprises a second header and a se-  
20 cond payload data block and has been generated due to a  
first data stream which comprises a first header and a  
first payload data block, wherein at least a part of the  
first header which comprises information regarding the ori-  
gin of the first data stream, is contained in the second  
25 header, the method comprising the following steps: extrac-  
ting the part of the first header from the second header;  
verifying the origin of the second data stream using the  
part of the first header which comprises information re-  
garding the origin of the first data stream; and in case of  
30 a positive result of the verifying step, playing the second  
data stream.

In accordance with a third aspect of the present invention,  
this object is achieved by an apparatus for generating a  
35 second data stream from a first data stream which comprises  
a first header and a first payload data block with payload  
data, the apparatus comprising the following: means for ex-  
tracting the first header from the first data stream; means  
for generating a second header for the second data stream;  
40 means for entering at least a part of the first header  
into the second header, the part of the first header in-

cluding information which allow conclusions as to the origin of the payload data; and means for generating a second payload data block which comprises the same payload data as the payload data block of the first data stream, so as to obtain the second data stream.

10 In accordance with a fourth aspect of the present invention, this object is achieved by an apparatus for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, at least a part of the first header, which comprises information regarding the origin of the first data stream, being contained in the second header, the apparatus comprising the following: means for extracting the part of the first header from the second header; means for verifying the origin of the second data stream using the part of the first header which comprises information regarding the origin of the first data stream; and means for playing the second data stream, which responds to the means for verifying, so as to play the second data stream only if the means for verifying provide a positive result.

The present invention is based on the knowledge that music piracy can only be limited by using a device-specific identification of payload data streams. This means that a payload data piece that has been processed in the form of a payload data stream is not licensed person-specific but device-specific. In order for such a system to find acceptance at the market the situation has to be taken into account that a person usually has several players and that a person wants to have a free choice on which player she/he wants to play the purchased multimedia piece.

It is pointed out at this stage that payload data in general includes multimedia data that is audio data, video



5 data or a combination of audio data and video data, but  
also text data. For practical reasons the subject matter of  
the present invention will be disclosed using multimedia  
data. It is however clear that all the payload data for  
which there is a demand to follow up their origin can be  
10 processed by the devices and methods according to the in-  
vention.

However, to prevent the way from being opened again for un-  
limited copying, a "copy" of the multimedia data stream has  
15 to be carried out device-specific for another device of a  
user as well. At the same time it is absolutely significant  
that the origin of each copy of a multimedia piece can be  
tracked down, i.e. it should always be possible to ascer-  
tain without doubt who has created a multimedia piece  
20 (author, composer), who has put it into circulation (pro-  
vider, distributor, supplier), who has made an intermediate  
copy, and who has possibly made a further intermediate  
copy, etc. Only when the origin is known a user of a multi-  
media piece can prove without doubt that he uses the multi-  
25 media piece legally, or only then an illegal user can be  
found guilty without doubt.

Furthermore it is possible to carry out the binding of the  
multimedia data not to one player directly, but to bind the  
30 data to a "Smart Card". Thereby identical multimedia data  
streams can be maintained on various devices, but can only  
be used on the respective device where the Smart Card is  
inserted at that time.

35 Therefore, according to the present invention a second data  
stream is generated from a first data stream comprising a  
first payload data block with multimedia data, that also

5 comprises a first header and a first payload data block  
with multimedia data, a second data stream is generated  
that also comprises again a header and a payload data  
block. However, in this second header, i.e. the header of  
the second data stream according to the present invention  
10 at least those parts of the first header, i.e. the header  
of the first data stream allowing conclusions as to the  
origin of the multimedia data are included. The second pay-  
load data block comprises the same multimedia data as the  
first payload data block, i.e. the payload data block of  
15 the first data stream.

The header of the second data stream can essentially have  
the same format as the header of the first data stream.  
However, it includes Besides the usual header information  
20 comprises additionally at least the information from the  
first header allowing conclusions as to the origin of the  
multimedia data.

Essentially, in a preferred embodiment of the present in-  
25 vention, the whole first header is entered into the second  
header. In order to protect the second header comprising  
the first header from manipulation it can additionally be  
provided with a digital signature that is derived from the  
data of the second (current) header and above that from the  
30 data of the first (old) header. In a preferred embodiment  
of the present invention, data from the first header allow-  
ing conclusions as to the origin of the multimedia data  
comprise a supplier identification, i.e. an identification  
of the supplier of the first data stream that could for ex-  
35 ample be the Deutsche Telekom (German telecommunications  
company), as well as author information allowing conclu-  
sions as to the author or composer, as well as a user iden-

5     tification, i.e. an identification of the device for which  
the data stream has originally been licensed.

It is a specific advantage of the inventive concept that it  
can be carried out as often as desired what leads to a mul-  
10     tiply recursive header structure since a third data stream  
that comprises a third header and a third payload data  
block again comprises origin information of the second  
header in its header. This origin information is on the one  
hand the origin information of the first header and on the  
15     other hand the origin information of the second header.  
Analogous to the origin information of the first header the  
origin information of the second header is for example an  
identification of the device the piece was originally li-  
censed for by the original supplier and an identification  
20     of the device a "copy" was made for, for example an identi-  
fication of a car hifi system.

Here, it will be especially noted that the author informa-  
tion of the first header is also present in the header of  
25     the third data stream. Thus, the inventive concept is in  
conformity with statutory regulations regarding any program  
or any apparatus removing author information as illegal.  
Such statutory regulations have already become national law  
in the United States and it might only be a question of  
30     time when these regulations will be nationalized Europe  
wide.

In a preferred embodiment of the present invention the part  
of an old header taken over into the new header contains  
35     only licensing information referring to the manner how a  
licensed multimedia piece may be used, i.e. how often it

5 may be played and how often it may be copied or whether a copy of a copy is legal or not.

The payload data block can of course be encrypted symmetrically, while the key of the symmetrical encrypting method  
10 is encrypted asymmetrically. In this case an apparatus for generating the second data stream will carry out a complete decryption from the first data stream and subsequently a complete new encryption.

15 Thus, the inventive concept allows full protection of a multimedia piece in a way from the author or composer via an arbitrary number of copies to an end user. Above that, the origin of a current copy can be tracked down unbrokenly at any time of a copy or distribution chain whereby the  
20 number of copies or distribution processes is arbitrary. Additionally, author information is considered any time whereby copyright protection is satisfied. Finally, the inventive concept can be implemented efficiently and flexible such that it is also suitable for inexpensive players with  
25 limited memory and processor resources, that it is easy to handle, and that modern client demands for high flexibility are fully considered.

#### Brief Description of the Drawings

30

Fig. 1 shows a multimedia data stream, which can be produced according to the present invention;

Fig. 2 shows a detailed illustration of the header and  
35 the payload data block of the encrypted multimedia data stream;

- 5    Fig. 3        shows a selection of certain entries into the individual sub blocks of the header block;
- Fig. 4        a schematic illustration of a distribution scenario;
- 10           Fig. 5        a schematic view of a data stream with recursive header structure;
- Fig. 6        a flow chart of a method for generating a second data stream from a first data stream according to the present invention; and
- 15           Fig. 7        a method for playing a second data stream generated based on a first data stream according to the present invention.
- 20

#### Detailed Description of Preferred Embodiments

- 25    Fig. 1 shows an encrypted multimedia data stream 10 comprising a header 12 and a payload data block 14 that is a block containing encrypted multimedia data. The payload data block 14 includes encrypted sections 16 and unencrypted sections 18 between the encrypted sections 16. In
- 30    addition a multimedia data stream, which can be produced according to the present invention, includes a further unencrypted section 20 following the header 12 and being arranged in front of an encrypted section 16.
- 35    Usually the multimedia data to be encrypted is encoded in any way, such as according to a MPEG standard, such as MPEG-2 AAC, MPEG-4 audio or MPEG Layer-3. It is thus suffi-

5     cient to encrypt certain sections of the multimedia data to  
be encrypted. This leads to an essentially decreased proc-  
essing expenditure both at the provider who encrypts the  
data and at the customer who in turn has to decrypt the  
data. Furthermore, the pleasure of hearing and seeing re-  
10   spectively of a user who only uses the unencrypted multime-  
dia data is seriously impaired by the constantly occurring  
encrypted blocks, when the multimedia data is only en-  
crypt ed partly.

15   Although Fig. 1 shows an encrypted multimedia data stream  
in which the header 12 is arranged at the beginning of the  
encrypted multimedia data stream this arrangement of the  
header and the payload data block is not to refer to the  
transmission of the encrypted multimedia data stream. The  
20   term "header" is only meant to express that a decryption  
device which is to decrypt the encrypted multimedia data  
stream at first requires at least parts of the header be-  
fore the multimedia data itself can be decrypted. Depending  
on the transmission medium the header may also be arranged  
25   at some place in the payload data block or be received af-  
ter certain parts of the payload data block when for exam-  
ple a packet-oriented transmission of the multimedia data  
stream is thought of, in which different packets, one of  
which may contain the header and another one a part of the  
30   payload data block, are transmitted via different physical  
transmission ways in such a way that the order of receipt  
does not have to correspond to the order of sending. How-  
ever, in this case a decryption device has to be able to  
save the packets received and to order them again in such a  
35   way that information is extracted from the header to begin  
the decryption. The encrypted multimedia data stream may  
further be present in the form of a file or also in the

5 form of an actual data stream, when for example a life transmission of a multimedia event is thought of. This application will especially occur with digital user-selective broadcasting.

10 The length of an encrypted section 16 is represented by a value amount 22 while the spacing in the encrypted multimedia data stream from the beginning of an encrypted section 16 to the beginning of the next encrypted section 16 is referred to as step 24. The length of the further encrypted

15 section 20 is given by a value first step 26.

These values 22, 24 and 26 are obviously required for a correct decrypting of the multimedia data in a decryption device. This is why they have to be entered into the header

20 12 as will be explained later.

Fig. 2 shows a more detailed illustration of the encrypted multimedia data stream 10 consisting of the header 12 and the payload data block 14. The header 12 is divided into

25 several sub blocks that will be explained especially referring to Fig. 3. It is pointed out that the number and the function of the sub blocks can be extended at will. Thus, in Fig. 2 some sub blocks of the header 12 are illustrated in an only exemplary way. The header includes as it is

30 shown in Fig. 2 a so-called crypt-block 29 comprising, in general terms, relevant information for encrypting the multimedia data. In addition the header 12 includes a so-called license block 30 comprising data referring to how a user can or is allowed to use the encrypted multimedia data

35 stream. The header 12 further includes a payload data info block 32 which can include information concerning the payload data block 14 and as well as general information about

5 the header 12 itself. Furthermore the header 12 may comprise an old header block 34 enabling a so-called recursive header structure. This block makes it possible for the user who, apart from a decryption device is also in the possession of an encryption device to reformat an encrypted multimedia data stream for other replay instruments in his possession without losing or modifying the original header information provided by the distributor. Depending on the application further sub blocks, such as an IP information block (IP = intellectual property) according to ISO/IEC 15 14496-1, MPEG-4, Systems, 1998, containing copyright information, can be added to the header 12.

As it is the standard in the art, an internal block structure can be allocated to each block, this structure at first requesting a block identifier and including the length of the sub block and at last giving the block payload data itself. Thus, the encrypted multimedia data stream, and in particular the header of the encrypted multimedia data stream, is given an increased flexibility in such a way that it can react to new requirements in such a way that additional sub blocks may be added or existing sub blocks may be omitted.

Fig. 3 gives an overview of the block payload data of the individual sub blocks shown in Fig. 2.

At the beginning the crypt block 28 is explained. It contains an entry for a multimedia data encryption algorithm 40 identifying the symmetrical encryption algorithm used in the preferred embodiment, which has been used when encrypting the multimedia data. The entry 40 can be an index for a table in such a way that, after reading the entry 40, a de-



5 encryption device is capable of selecting this encryption algorithm the encryption device has used from a plurality of encryption algorithms. The crypt block 28 further includes the entry first step 26, the entry step 24 and the entry amount 22, which has already been illustrated in connection  
10 with Fig. 1. These entries in the header enable a decryption device to subdivide an encrypted multimedia data stream accordingly to be able to carry out a correct decryption.

15 The crypt block 28 further contains an entry for the distributor or provider or supplier 42, the entry being a code for the distributor who has produced the encrypted multimedia data stream. An entry user 44 identifies the user who has obtained the encrypted multimedia data stream in some  
20 way from the distributor who is identified by the entry 42. According to the invention it is preferred not to use a person-related user identification since this would open the way for illegal copies. Instead it is preferred to carry out the user identification device specific. The entry user would then for example comprise the serial number  
25 of a PC, a laptop, a car hifi system, a home stereo system, smart card etc. that authorizes playing only on a certain device. For further increase of flexibility and/or safety a certain identification like for example a logic link of the  
30 hard disk size with the processor number etc. for the example of a PC can be applied instead of a serial number that looks different for every producer but might by chance be identical.

35 An entry 46 contains an output value that will be discussed in detail later. This output value in general represents an encrypted version of the multimedia data key which, in con-

5    nection with the multimedia data encryption algorithm identified by the entry 40, is required to decrypt the encrypted multimedia data (sections 16 in Fig. 1) present in the payload data block 14 correctly. In order to achieve a sufficient flexibility for future applications, the two entries output value length 48 and output value mask 50 are  
10    further provided. The entry output value length 48 illustrates the actual length of the output value 46. To achieve a flexible header format more bytes are however provided in the header format, for the output value than an output  
15    value actually comprises. The output value mask 50 thus illustrates how a shorter output value is distributed in a way on a longer output value place. If the output value length is for example half as big as the space available for the output value, the output value mask could be formed  
20    in such a way that the first half of the output value mask is set while the second half is masked. In this case the output value would simply be entered into the space provided for the header by the syntax and occupy the first half while the other half would be ignored due to the out-  
25    put value mask 50.

Now the license block 30 of the header 12 will be explained. The license block includes an entry bit mask 52. This entry can comprise certain specific information for  
30 replaying or for the general way of using the encrypted multimedia data. With this entry a decryption device could especially be told whether the payload data can be replayed locally or not. In addition at this point it may be signalled whether the challenge response method has been used  
35 for the encryption, this method being described in the already mentioned German patent DE 196 25 635 C1 and enabling an efficient data base access.

5

An entry expiration date 54 indicates the point in time at which the permission to decrypt the encrypted multimedia data stream expires. A decryption device will in this case check the entry expiration date 54 and compare it to a  
10 build-in time measuring device in order not to carry out a decryption of the encrypted multimedia data stream if the expiration date has been exceeded. This makes it possible for the provider to make encrypted multimedia data available for a limited amount of time, which has the advantage  
15 of a much more flexible handling and price setting. This flexibility is further supported by an entry starting date 56 in which it is specified from which point on an encrypted multimedia file is allowed to be decrypted. An encryption device will compare the entry starting date with  
20 its built-in watch to only carry out a decryption of the encrypted multimedia data when the current point in time is later than the starting date 56.

The entry allowed replay number 58 indicates how often the  
25 encrypted multimedia data stream can be decrypted, that is replayed. This further increases the flexibility of the provider in such a way that it for example only allows a certain number of replays compared to a certain sum which is smaller than a sum which would arise for the unlimited  
30 usage of the encrypted multimedia data stream.

For verifying and supporting respectively the entry allowed  
replay number 58 the license block 30 further includes an  
entry actual replay number 60 which could be incremented by  
35 one for example after each decryption of the encrypted multimedia data stream. A decryption device will thus always check whether the entry actual replay number is smaller

5 than the entry allowed replay number. If this is the case,  
a decryption of the multimedia data is carried out. If this  
is not the case, a decryption is no longer carried out.

10 Analog to the entries 58 and 60 entries allowed copy num-  
bers 62 and actual copy number 64 are implemented. By means  
of the two entries 62 and 64 it is made sure that a user of  
the multimedia data only copies them as often as he or she  
is allowed to do so by the provider or as often as he or  
she has paid for when purchasing the multimedia data. By  
15 the entries 58 to 64 a more effective copyright protection  
is assured, a selection between private users and indus-  
trial users being attainable for example by setting the en-  
tries allowed replay number 58 and allowed copy numbers 62  
to a smaller value.

20

The licensing could for example be designed in such a way  
that a certain number of copies (entry 62) of the original  
are allowed while copies of a copy are not allowed. The  
header of a copy would then, unlike the header of the  
25 original, have zero as the entry allowed copy number in  
such a way that a proper encryption/decryption device can  
no longer copy this copy.

In the example for a multimedia data protection protocol  
30 (MMP) shown here the header 12 further contains a payload  
data information block 32 having in this case only two  
block payload data entries 66 and 68, the entry 66 contain-  
ing a hash sum on the total header, while the entry 68  
identifies the type of hash algorithm having been used for  
35 forming the hash sum on the total header.



5 For this purpose author information (IP information block)  
could for example count prior user information and dis-  
tributor information which enables tracing back of a multi-  
media file which for example has been decrypted and en-  
crypted several times by different instruments to the  
10 original provider transparently, the author information be-  
ing maintained. It is thus possible to check at any point  
whether an encrypted multimedia file has been acquired le-  
gally or illegally.

15 Fig. 4 shows a schematic block diagram of a scenario  
wherein the inventive concept can be applied in an advanta-  
geous way. An author or composer 100 has created a multime-  
dia piece, for example a text, a piece of music, a film or  
a picture. He delivers this work, in this invention gener-  
20 ally referred to as multimedia piece, to a supplier 102 of  
multimedia data. It is especially pointed out here that the  
expression "multimedia data" in the sense of the present  
invention comprises audio data, video data or a combination  
of audio and video data.

25 The supplier ensures that the multimedia piece of the  
author/composer 100 is put in circulation by encoding it  
for example according to the method MPEG layer 3 (MP3). In  
order to achieve a customer selective providing for use of  
30 the encoded multimedia piece the supplier 102 will bring  
the encoded multimedia piece into a first data stream com-  
prising a header and payload data block. A data stream as  
it might be used is illustrated in Fig. 3.

35 In this connection it should be especially pointed to the  
IP information block 72 comprising author information 74 as  
payload data identifying the author/composer or in general

5 artist. The IP information block could for example be carried out according to ISO/IEC 14496-1 MPEG-4 systems, 1998. It could especially comprise the name of the author/composer/artist or also the ISBN number (ISBN = international standard book number), the ISRC code (ISRC =  
10 international standard recording code), the ISAN number (ISAN = international standard audiovisual number), the ISMN number (ISMN = international standard music number), etc. Such meta information will allow a unique identification of the author of the multimedia piece such that by  
15 adding these meta information to the payload data the enforcement of copyrights will be much easier.

The supplier of multimedia data 102 generates a first data stream comprising a first header and a first payload data  
20 block. All the data illustrated in Fig. 3 can be included in the header, wherein the author information (entry 74), the distributor identification (entry 42) and the user identification (entry 44) should be especially noted. While the author information (entry 74) represents the origin of  
25 the multimedia piece in general, the distributor identification (42) uniquely defines the origin of the first data stream while the user identification defines the "destination" of the first data stream, i.e. the device that is allowed to use the data stream and that has also paid for it,  
30 whereby on the one hand the service of the supplier 102 of multimedia data is paid and on the other hand royalties to the author/composer 100 can flow. In the first header of the first data stream a receiver-PC 104 could for example be identified by the user identification 44. The first data  
35 stream can now on the one hand be played on the receiver-PC 104, however, according to the invention, the receiver-PC is defined in such a way that it can also generate a "copy"

5 of the first data stream in order to generate one or several second data streams comprising in their header the user identification 44 of a car hifi system 106a, a home hifi system 106b, a solid state player 106c, etc.

10 Every second header will essentially comprise the same payload data block, the header of every second data stream, i.e. the second header, will however be different regarding the user identification 44. However, according to the invention, every second header will comprise information al-

15 lowing conclusions as to the origin of the respective second data stream. This information can comprise author information, an identification for the receiver-PC 104 and an identification for the supplier 102 of the first data stream. Preferably, the second header additionally com-

20 prises licence information referring to the fact how often the multimedia piece may be played or how often it may be copied. It can especially happen that for example five copies are allowed but no copy of the copy is allowed. In the entry allowed copy number 62 of the first header there

25 would for example be five. In the entry allowed copy number of the second header however, there would be zero. Even when the car hifi system 106a, the home hifi system 106b or the solid state player 106c were designed in such a way that it can carry out a decryption or an encryption by it-

30 self, i.e. like the receiver-PC 104, still no further copy would be produced, i.e. no third data stream, since the entry 62 in the second header of the second data stream is set to zero. If this were not the case and if the copy of a copy were allowed the devices 106a to 106c could again cre-

35 ate third data streams but would comprise origin information of the respective second data stream and naturally of the respective first data stream.



5 This results in a recursive header structure shown schematically in Fig. 5 that can principally be repeated arbitrarily. Fig. 5 shows an nth data stream 110 comprising an nth header 112 and an nth payload data block 114. The nth  
10 header 112 again comprises a (n-1)th header that again comprises a (n-2)th header, etc.

Preferably, the supplier of multimedia data 102 (Fig. 4) encrypts the multimedia data in the first payload data block at least in parts. Preferably, a symmetrical encrypting method for encrypting the multimedia data is used, wherein the key of the symmetrical encrypting method is again encrypted asymmetrically. The asymmetric key encrypted with the private key of the supplier 102 for the symmetrical encrypting method is the output value 46 (Fig. 3). The receiver-PC 104 will therefore need the respective public key of the supplier 102 of multimedia data in order to decrypt the output value 46 again, in order to obtain the key for the symmetrical decrypting method that the supplier 102 of multimedia data has used as well. The receiver-PC 104 is now enabled to play the first data stream. If the first data stream is encoded the receiver-PC 104 carries out a decoding prior to playing. The sequence will therefore be: decrypting, decoding, and playing.

30 However, the receiver-PC should also be able to generate a second data stream for a specific additional player 106a to 106c. In this case the receiver-PC 104 can be configured for encrypting the multimedia data that are decrypted, 35 wherein a symmetrical encrypting method is preferred due to speed aspects. The receiver-PC 104 will again asymmetri- cally encrypt the key for the symmetrical encrypting method

5 with its private key, provide the second header with its own identification as distributor entry 42 and further provide the second header with the identification for example of the car hifi system as user identification 44. Further, the receiver-PC 104, will generate a different output value  
10 that will be entered into the entry 46 of the second header since the receiver-PC has a different data key than the supplier 102 of multimedia data. Above that, the receiver-PC will update the licence-block of the second header as desired. However, according to the invention, it will preferably  
15 erably write the whole first header into the entry old header 70 in such a way that all information of the first header are maintained and especially the origin information of the first data stream as it has been described several times.

20

Neither the first, second or the nth header are encrypted themselves. In order to protect the respective headers from attacks after the completion e.g. of the second header a hash sum is formed on the header for example according to a  
25 hash algorithm identified in entry 68 (Fig. 3). Preferably, this hash sum is not only formed by the blocks 28, 30, 32, 72 of the second header but it also comprises the block for the old header 34. This hash sum can then be directly entered into the entry 66 (Fig. 3). For the increase of  
30 safety it is however preferred to enter a digital signature for the hash sum of the second header. A digital signature of the hash sum on the second header could for example be again formed with an asymmetrical encryption method in such a way that the receiver-PC 104 generating the second data  
35 stream encrypts the hash sum on the second header with its own private key and writes the result into the entry 66.

5 The home hifi system 106b will now at first verify the second data stream by also forming a hash sum on the second header as it is supplied to the home hifi system. Further, the home hifi system 106b will decrypt the entry 66 in the second header with the public key of the receiver-PC 104  
10 and compare the obtained result with the just calculated hash sum. If both hash sums are the same it can be assumed that the second data stream has not been manipulated. If the two results differ, a legally implemented car hifi system will not continue playing since it can be assumed that  
15 unallowed manipulations have been carried out either at the second header or in a way "belated" at the first header.

Fig. 6 shows a flow chart for the inventive method for generating a second data stream from a first data stream that  
20 is carried out by the receiver-PC 104 in order to "retag" the device specifically licensed first data stream to other devices (106a to 106c).

Basically, the receiver-PC 104 will at first extract the  
25 header from the first data stream (116). Above that, the receiver-PC 104 will generate a second header for the second data stream (118) as far as possible. This header generated as far as possible could comprise all information of the header shown in fig. 3 (blocks 28, 30, 32, 34, 72), but  
30 not the old header block 34. This block will be described in a step 120, wherein at least the origin information from the first header is entered into the entry 70. However, for safety reasons and also for implementation reasons it is preferred to enter not only the origin information from the  
35 first header but also all information from the first header into the entry 70 of the second header. This could lead to the fact that certain information exist twice, like e.g.

5 the author information 74 as well as information from other blocks, for example first step 26, step 24, amount 22, etc. Already here it can be seen that by the fact that the receiver-PC 104 generates a complete second header in step 118 it is not bound to the parameters of the supplier 102  
10 of multimedia data. For example, a less expensive encrypting method could be applied in order to enable the second data stream to be encrypted with less effort again for example by the solid state player 106c that needs, as known, limited memory and processor resources in order to be offered  
15 inexpensively. Considering these aspects the payload data block of the second data stream might even not be encrypted anymore at all, if preferred.

Finally, the receiver-PC 104 generates a second payload  
20 data block for the second data stream (122) in order to finally obtain the second data stream.

The flow chart in Fig. 7 describes in general a method for playing a second data stream generated based on a first  
25 data stream, wherein this method could be carried out in one of the devices 106a to 106c. If between the supplier 102 of multimedia data and the receiver-PC 104 a further intermediate distributor as for example a "retailer" of multimedia data is disposed whom the supplier 102 of multimedia data who will then have a wholesaler function supplies, the inventive method generally illustrated in Fig. 7  
30 would already be carried out by the receiver-PC 104.

Generally, the method for playing can be started with the  
35 step of reading the second header of the second data stream (130). The device 106a will then for example extract the part of the first header comprising origin information,

5 i.e. the old header block 34 and read the payload data of  
the entry 70 (132).

In order to prevent the playing of illegal pieces the ori-  
gin of the second data stream is verified in step 134 using  
10 the origin information in entry 70. Such a verification  
could for example consist of checking whether origin infor-  
mation is present in the second header at all (136). If it  
is found out in the verification 136 that no origin infor-  
mation is present in the second header at all, a legally  
15 driven playing apparatus according to the present invention  
will refuse playing and will stop the operation (138). If  
it is found out in this simple form of verification 136  
that origin information is present and that it makes sense  
and is no "deception data" of some sort, the inventive  
20 playing apparatus will begin or continue playing the second  
data stream (140).

A more expensive way of verification could be to test  
whether the supplier identification 42 of the second header  
25 matches the user identification 44 of the first header. In  
this case it would be proved without doubt that the copy  
present in the player comes from the respective home-PC.  
Any further verification techniques with more or less ef-  
fort are considered.

30

In a preferred embodiment of the present invention it is  
preferred to carry out the verification via a digital sig-  
nature comprising both data of the first header and data of  
the second header, as it has been described in connection  
35 with Fig. 4. Further even more complicated methods can also  
be used for verification wherein however always the origin  
of the present data stream is tested that can either be

- 5 author information or other respective supplier entries 42  
or user entries 44 of the individually embedded header of  
the generally spoken multiply recursive header structure  
that is illustrated in Fig. 5.
- 10 Besides the verification of the origin of the second data  
stream (step 134 in Fig. 7) the player will preferable be  
implemented in such a way that it processes also the li-  
cense block 30 and especially for example according to the  
entries 58 and 60 processes regarding to the authorized or  
15 actual playing number in order to find out whether it may  
play a data stream. The player will of course use the other  
information of the second header in the described manner if  
the second data stream is encrypted in order to finally de-  
crypt, decode and play the second data stream.

5

Claims

1. Method for generating a second data stream from a first data stream which comprises a first header and a first payload data block with payload data, the method comprising the following steps:

10 extracting the first header from the first data stream;

15 generating a second header for the second data stream;

entering at least a part of the first header into the second header, the part of the first header including information which allows conclusions as to the origin of the payload data; and

20 generating a second payload data block having the same payload data as the payload data block of the first data stream, so as to obtain the second data stream.

25

2. Method as claimed in claim 1, wherein the information allowing conclusions as to the origin of the first data stream includes an identification for a supplier of the first data stream.

30

3. Method as claimed in claim 1, wherein the information allowing conclusions as to the origin of the first data stream includes author information, such as the author, the component, the ISRC number, the ISAN number or the ISMN number of the payload data of the first data stream.

35

4. Method as claimed in claim 1, wherein the part of the first header, which is entered into the second header, further comprises an identification of the receiver of the first data stream.

40

- 5     5.     Method as claimed in claim 4, wherein the identification is device-specific, and the receiver of the first data stream is a player indicated by the identification, or a smart card.
- 10    6.     Method as claimed in claim 1, wherein the part of the first header which is entered into the second header further comprises licence data relating to the manner in which a receiver of the first data stream may use the same, the licence data of the first header specifying the licence data of the second header.
- 15
7.     Method as claimed in claim 6, wherein the licence data of the first header specify that the first data stream may be copied a certain number of times, that no copy may be taken of a copy, however, the step of generating the second header for the second data stream including the entering of second licence information into the second header of the second data stream, such that no more copy may be taken of the second data stream.
- 20
- 25    8.     Method as claimed in claim 4,
- wherein the step of generating a second header comprises the step of entering an identification for the receiver of the second data stream as a user identification, and of entering an identification of the receiver of the first data stream as a supplier identification, and
- 30
- 35     wherein the step of entering at least a part of the first header into the second header comprises the entering of the identification of the supplier of the first data stream as a supplier identification, and the entering of the identification of the receiver of the first data stream as a user identification into a part of the second header, which is reserved for information of the first header.
- 40



- 5
9. Method as claimed in claim 1, which further comprises the following step:
- 10
- issuing a digital signature for the second header, including the part of the first header, and attaching the digital signature to the second header.
10. Method as claimed in claim 9, wherein the issuing step further comprises the following substeps:
- 15
- forming a hash sum over the second header, including the part of the first header, using a specified hash algorithm; and
- 20
- encrypting the hash sum by means of an asymmetric encrypting method using a private key of the receiver of the first data stream.
11. Method as claimed in claim 1, wherein the payload data
- 25
- in the payload data block are at least partly encrypted and wherein encrypting information is contained in the first header, the step of generating the second header further comprising the following steps:
- 30
- decrypting the first payload data block of the first data stream using the encrypting information in the first header;
- 35
- encrypting the decrypted payload data and entering corresponding encrypting information into the second header,
- the encrypting information of the first header also being entered into the second header.
- 40
12. Method as claimed in claim 11, wherein the encrypted payload data in the first payload data block are en-

5        encrypted symmetrically and wherein the key is again encrypted asymmetrically using a private key, the decrypting step comprising the following steps:

10        decrypting the encrypted key by means of the public key of the supplier so as to obtain the key for a symmetric decryption;

15        encrypting a payload data key of the decrypted payload data using a private key of a receiver of the first data stream carrying out the method for generating a second data stream; and

20        entering the asymmetrically encrypted payload data key into the second header.

13. Method as claimed in claim 1, wherein in the step of entering, the entire first header is entered into the second header.

25    14. Method as claimed in claim 1, wherein the first header itself comprises at least a part of a header of a data stream which relates to the origin of the first data stream, such that the entering step results in a multiply recursive header structure.

30    15. Method for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, wherein at least a part of the first header which comprises information regarding the origin of the first data stream, is contained in the second header, the method comprising the following steps:

40        extracting the part of the first header from the second header;

- 5        verifying the origin of the second data stream using  
the part of the first header which comprises informa-  
tion regarding the origin of the first data stream;  
and
- 10        in case of a positive result of the verifying step,  
playing the second data stream.
16.    Method as claimed in claim 15, wherein the second  
header of the second data stream has a digital signa-  
15        ture attached to it which fits the part of the first  
header, and wherein the verifying step comprises the  
following substep:
- 20        checking the authenticity of the second header using  
the digital signature.
17.    Method as claimed in claim 16, wherein the digital  
signature is the result of an encryption of a hash sum  
of the second header, which encryption has been car-  
25        ried out by means of a private key of the apparatus  
having generated the second data stream, the step of  
checking the authenticity comprising the following  
steps:
- 30        decrypting the digital signature by a public key of  
the apparatus which has generated the second data  
stream, so as to obtain the hash sum of the second  
header;
- 35        forming a hash sum of the present header;
- 40        comparing the hash sums;
- in case of the hash sums matching, issuing a positive  
verification result.

5 18. Method as claimed in claim 17, wherein the part of  
the first header further comprises licence information  
regarding the manner in which the first data stream  
may be utilized, and wherein the second header com-  
prises licence data derived from the licence data of  
10 the first header, the method further comprising the  
following substeps:

comparing the licence data of the second header and  
the first header so as to evaluate the authenticity of  
15 the licence data of the second header;

in case of questionable authenticity, blocking the  
playing of the second data stream.

20 19. Apparatus for generating a second data stream from a  
first data stream which comprises a first header and a  
first payload data block with payload data, the appa-  
ratus comprising the following:

25 means for extracting the first header from the first  
data stream;

means for generating a second header for the second  
data stream;

30 means for entering at least a part of the first  
header into the second header, the part of the first  
header including information which allow conclusions  
as to the origin of the payload data; and

35 means for generating a second payload data block which  
comprises the same payload data as the payload data  
block of the first data stream, so as to obtain the  
second data stream.

40 20. Apparatus as claimed in claim 19, which is designed as  
a personal computer.

- 5
21. Apparatus for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, at least a part of the first header, which
- 10 comprises information regarding the origin of the first data stream, being contained in the second header, the apparatus comprising the following:
- 15 means for extracting the part of the first header from the second header;
- means for verifying the origin of the second data stream using the part of the first header which comprises information regarding the origin of the first
- 20 data stream; and
- means for playing the second data stream, which responds to the means for verifying, so as to play the second data stream only if the means for verifying
- 25 provide a positive result.
22. Apparatus as claimed in claim 21, which is designed as a hifi system, as a car hifi system, as a portable multimedia player, as a computer or as a component of
- 30 any of the above-mentioned devices.

**Method and Apparatus for Generating a Data Stream and  
Method and Apparatus for Playing a Data Stream**

Abstract

In a method for generating a second data stream from a first data stream, which comprises a first header and a first payload data block with payload data, the first header is initially extracted from the first data stream. Subsequently the second header for the second data stream is generated. Then, at least a part of the first header is entered into the second header, the part of the first header including information, which allows conclusions as to the origin of the payload data. Finally, the second payload data block is generated, which comprises the same payload data, so as to obtain the complete second data stream. The method according to the invention enables device-specific encrypting of payload data, a flexible, device-specific "copy" for other devices of a user and, in particular, complete documentation of the origin of the present copy, such that effective copyright protection may be realized.

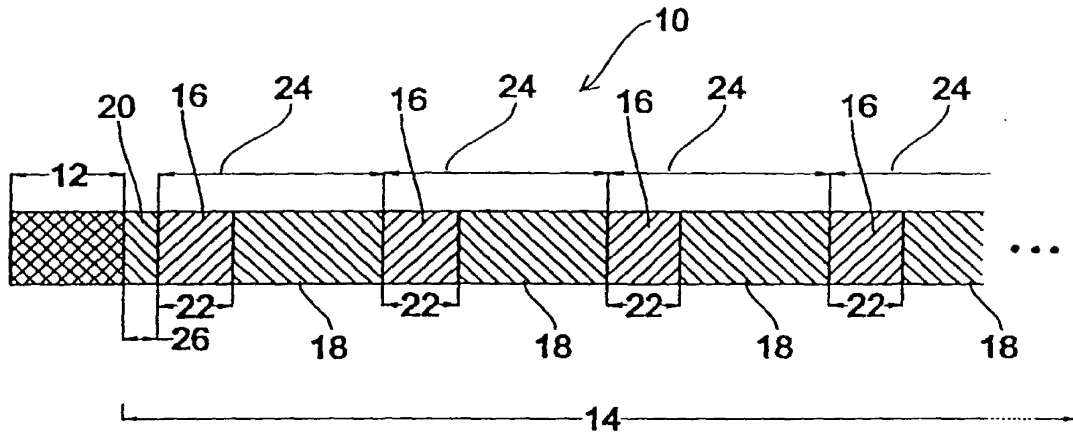


Fig. 1

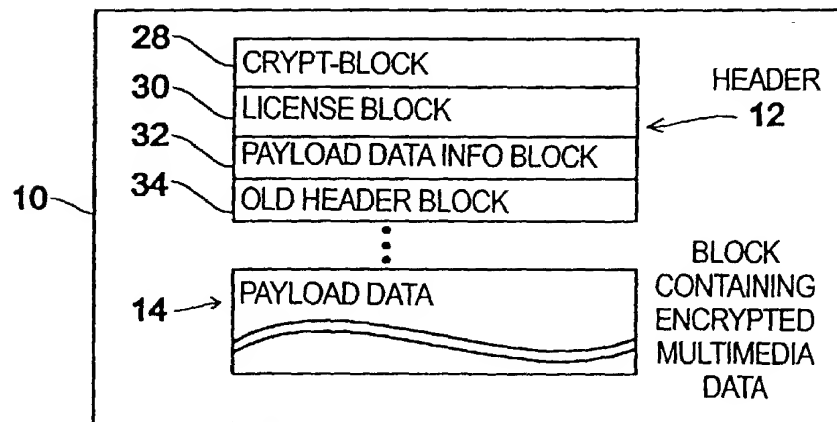


Fig. 2

107

28	CRYPT BLOCK	MMD ENCRYPTION ALGORITHM		40
		FIRST STEP		26
		STEP		24
		AMOUNT		22
		DISTRIBUTOR		42
		USER		44
		OUTPUT VALUE LENGTH		48
		OUTPUT VALUE MASK		50
		OUTPUT VALUE	X	46
30	LICENSE BLOCK	BIT MASK		52
		EXPIRATION DATE		54
		STARTING DATE		56
		ALLOWED REPLAY NUMBER		58
		ACTUAL REPLAY NUMBER	X	60
		ALLOWED COPY NUMBER		62
		ACTUAL COPY NUMBER	X	64
32	PAYLOAD DATA INFO BLOCK	HASH SUM ON HEADER	X	66
		TYPE OF HASH ALGORITHM		68
34	OLD HEADER BLOCK	OLD HEADER	X	70
34	IP INFORMATION BLOCK	AUTHOR INFORMATION		74
72	PAYLOAD DATA BLOCK			
		PAYLOAD DATA TYPE		
		PAYLOAD DATA		
14				

Fig. 3



- 3/5 -

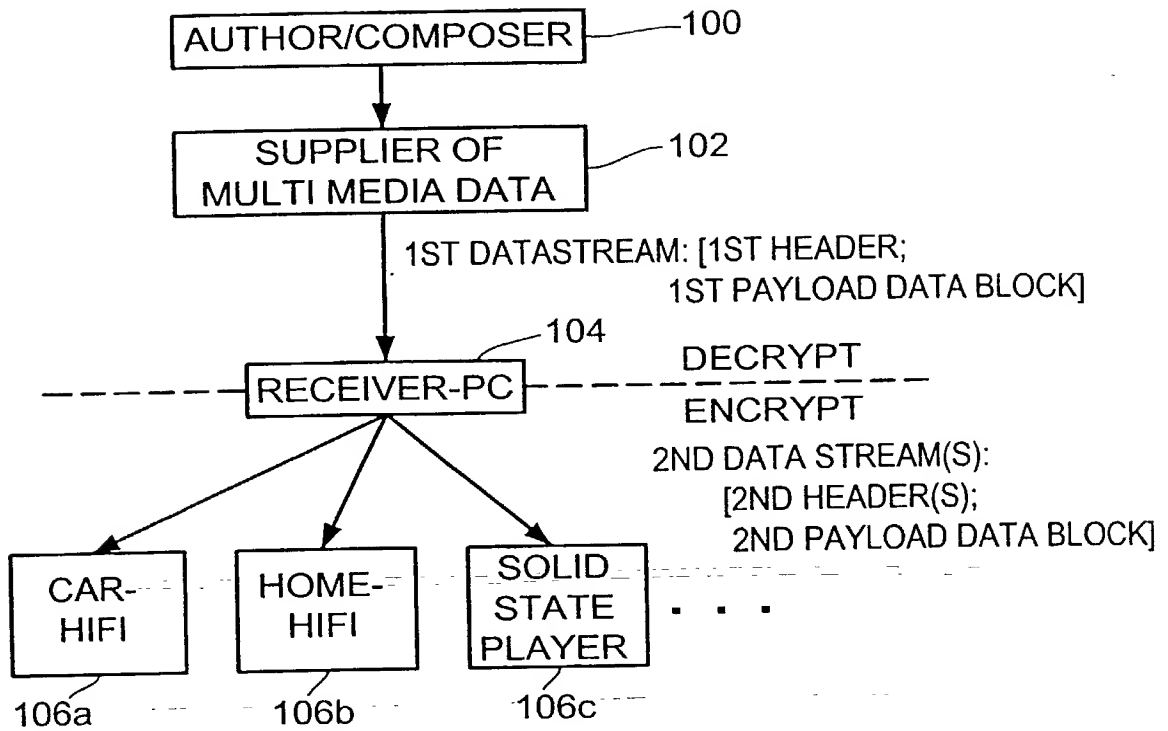


Fig. 4

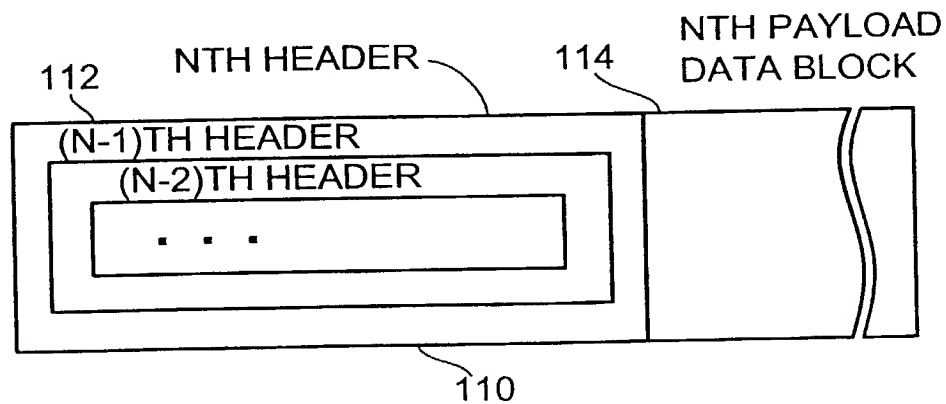


Fig. 5

- 4/5 -

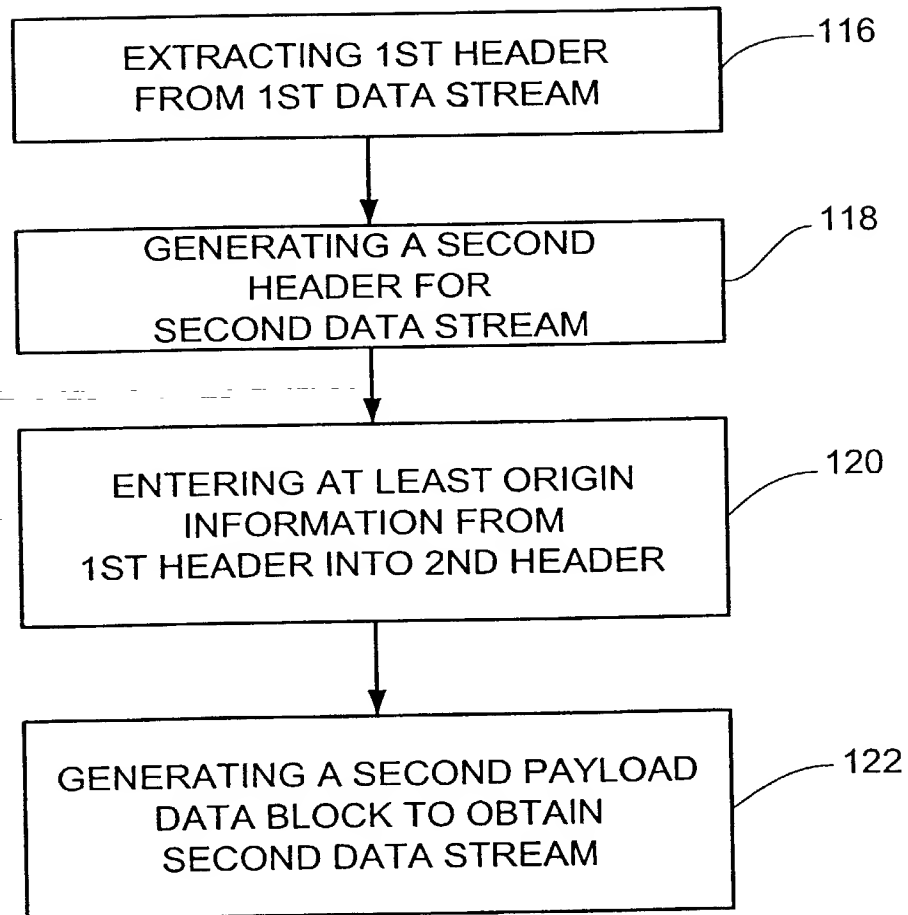


Fig. 6

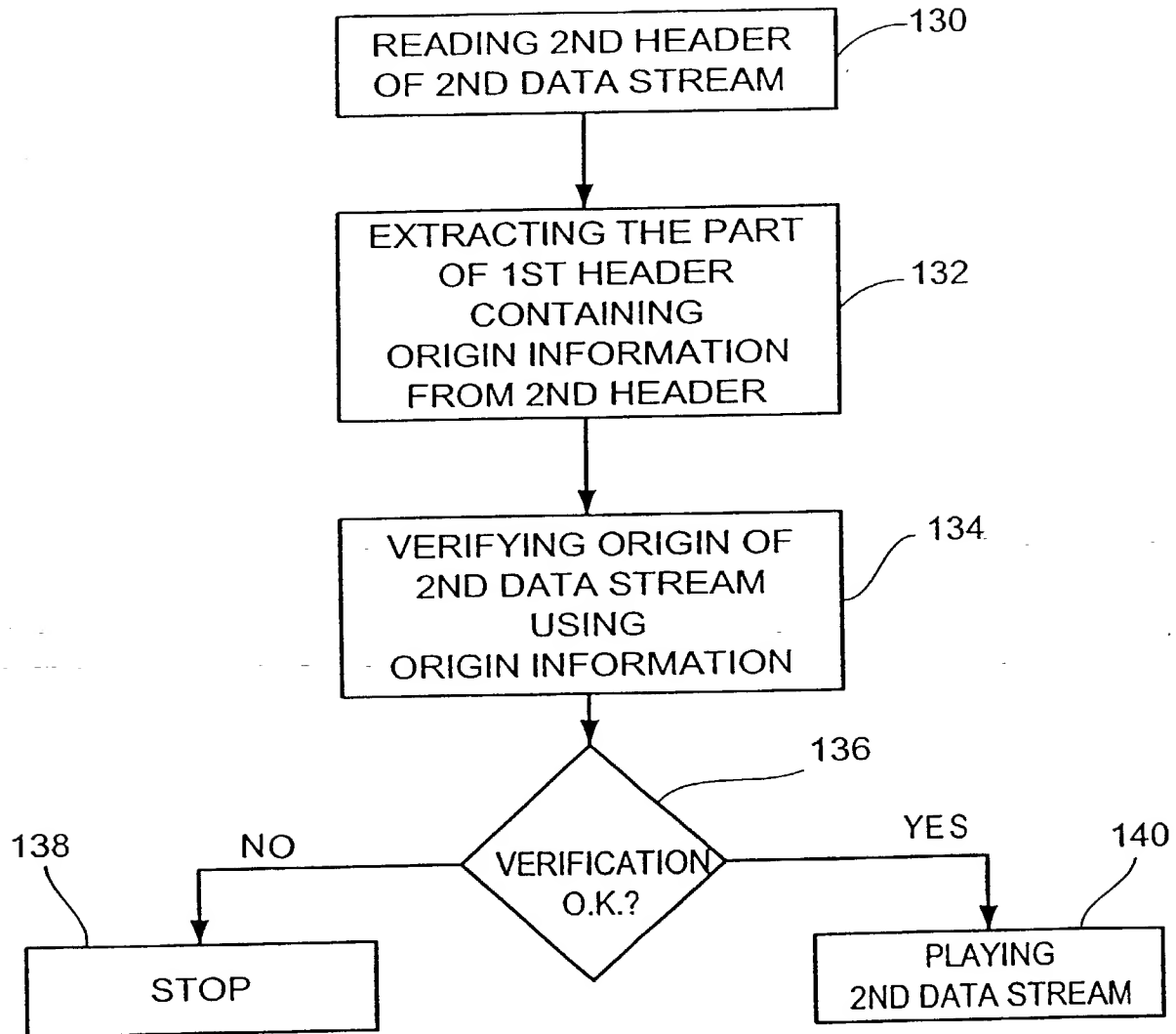


Fig. 7

09/913690

531 Rec'd PCT. 16 AUG 2001

National Phase of PCT/EP99/09980 in U.S.A.

Title: Method and Apparatus for Generating a Data Stream and  
Method and Apparatus for Playing a Data Stream

Applicants: RUMP, Niels et al.

---

Annotated copy of Final version of PCT/EP99/09980

---

5       **Method and Apparatus for Generating a Data Stream and**  
          **Method and Apparatus for Playing a Data Stream**

Description

10               Field of the Invention

The present invention relates to the encryption or decryption of payload data, like e.g. audio and/or video data and especially to audio and/or video data present in the form of a data stream comprising a header and a payload data block.

Background of the Invention and Prior Art

20

With the occurrence of telecommunication networks and in particular due to the huge spreading of multimedia data-capable personal computers and, most recently, of so-called solid state players, a need has arisen to market digital multimedia data, such as digital audio data and/or digital video data, commercially. Telecommunication networks for example can be analog telephone lines, digital telephone lines, such as ISDN, or the Internet. Among the commercial providers of multimedia products there is a need to sell or lend multimedia data, wherein it should be possible for a costumer to be able to select a certain product individually at any time from a certain catalogue, this product then of course being only allowed to be used by the costumer who has paid for it.

35

Unlike well-known encrypted television programs, such as the television channel Premiere, in which the emitted data

5 is encrypted in the same way for all users who have acquired a suitable decryption device by paying a certain charge, the present invention is to provide methods and devices enabling an individual, customer-selective and safe encryption and decryption of multimedia data. Unlike the  
10 television channels mentioned above which give a fixed program all of which the user has to decide for, the methods and devices of the present invention enable a maximum freedom of selection for the user, which means that the user has only to pay for those products he or she actually wants  
15 to use.

DE 196 25 635 C1 describes methods and devices for encrypting and decrypting multimedia data, the multimedia data being present in the form of an encrypted multimedia file  
20 comprising a destination data block and a payload data block. Parts of the destination data block and at least some parts of the payload data block are encrypted by means of different keys, especially symmetrical encryption methods being used.

25 Further, in the method for encrypting or decrypting multimedia data described in DE 196 256 35 C1 a user index is entered into a determination data block of a bitstream with encrypted multimedia data that identifies the user authorized to use an encrypted multimedia data stream. If this  
30 user index identifies merely one person, this method is only safe against unauthorized copying if that person who has purchased an encrypted multimedia data stream acts correctly and legally. This can, however, not always be guaranteed. If the person who has purchased an encrypted multimedia data stream legally carries out copying, it will not  
35 be possible to see from a copy who has copied it. The ori-

5 gin of the copy can therefore not be tracked down anymore  
which will open the way for violations of copyrights, in-  
correct behaviour assumed.

10 However, if the user index does , not only identify the  
user as a person but a specific player of a user, like e.g.  
the PC of the user, a safety is achieved in such a way that  
the user can play the encrypted multimedia data stream only  
on the player identified by the user index regardless  
whether the user behaves legally or illegally.

15 However, the problem with this solution is the fact that it  
is not flexible, i.e. it dictates the user where he has to  
play the purchased multimedia data stream due to the copy-  
right protection. There is not a lot of imagination needed  
20 to predict that such system will only find little accep-  
tance at the market especially when thinking about the fact  
that a number of players exist in a normal household. Such  
players can include for example a personal computer, a lap-  
top, a hifi system, a car hifi system, a video recorder, a  
25 solid state player, etc.

### Summary of the Invention

30 Therefore, it is the object of the present invention to  
provide a flexible concept for selectively providing multi-  
media data that on the one hand finds acceptance at the  
market and at the other hand takes copyright aspects into  
consideration.

35 ~~This object is achieved by a method for generating a second  
data stream from a first data stream according to claim 1,~~

5 ~~by a method for playing a second data stream generated~~  
~~based on a first data stream according to claim 15, by an~~  
~~apparatus for generating a second data stream from a first~~  
~~data stream according to claim 19, and by an apparatus for~~  
~~playing a second data stream generated based on a first~~  
10 ~~data stream according to claim 21.~~

In accordance with a first aspect of the present invention,  
this object is achieved by a method for generating a second  
data stream from a first data stream which comprises a  
15 first header and a first payload data block with payload  
data, the method comprising the following steps: extracting  
the first header from the first data stream; generating a  
second header for the second data stream; entering at least  
a part of the first header into the second header, the part  
20 of the first header including information which allows con-  
clusions as to the origin of the payload data; and generat-  
ing a second payload data block having the same payload  
data as the payload data block of the first data stream, so  
as to obtain the second data stream.

25 In accordance with a second aspect of the present inven-  
tion, this object is achieved by a method for playing a se-  
cond data stream which comprises a second header and a se-  
cond payload data block and has been generated due to a  
30 first data stream which comprises a first header and a  
first payload data block, wherein at least a part of the  
first header which comprises information regarding the ori-  
gin of the first data stream, is contained in the second  
header, the method comprising the following steps: extrac-  
35 ting the part of the first header from the second header;  
verifying the origin of the second data stream using the  
part of the first header which comprises information re-  
garding the origin of the first data stream; and in case of  
a positive result of the verifying step, playing the second  
40 data stream.



5 In accordance with a third aspect of the present invention,  
this object is achieved by an apparatus for generating a  
second data stream from a first data stream which comprises  
a first header and a first payload data block with payload  
data, the apparatus comprising the following: means for ex-  
10 tracting the first header from the first data stream; means  
for generating a second header for the second data stream;  
means for entering at least a part of the first header  
into the second header, the part of the first header in-  
cluding information which allow conclusions as to the ori-  
15 gin of the payload data; and means for generating a second  
payload data block which comprises the same payload data as  
the payload data block of the first data stream, so as to  
obtain the second data stream.

20 In accordance with a fourth aspect of the present inven-  
tion, this object is achieved by an apparatus for playing a  
second data stream which comprises a second header and a  
second payload data block and has been generated due to a  
first data stream which comprises a first header and a  
25 first payload data block, at least a part of the first hea-  
der, which comprises information regarding the origin of  
the first data stream, being contained in the second hea-  
der, the apparatus comprising the following: means for ex-  
tracting the part of the first header from the second hea-  
30 der; means for verifying the origin of the second data  
stream using the part of the first header which comprises  
information regarding the origin of the first data stream;  
and means for playing the second data stream, which re-  
sponds to the means for verifying, so as to play the second  
35 data stream only if the means for verifying provide a posi-  
tive result.

The present invention is based on the knowledge that music  
piracy can only be limited by using a device-specific iden-  
40 tification of payload data streams. This means that a pay-  
load data piece that has been processed in the form of a

5 payload data stream is not licensed person-specific but device-specific. In order for such a system to find acceptance at the market the situation has to be taken into account that a person usually has several players and that a person wants to have a free choice on which player she/he  
10 wants to play the purchased multimedia piece.

It is pointed out at this stage that payload data in general includes multimedia data that is audio data, video data or a combination of audio data and video data, but  
15 also text data. For practical reasons the subject matter of the present invention will be disclosed using multimedia data. It is however clear that all the payload data for which there is a demand to follow up their origin can be processed by the devices and methods according to the invention.  
20

However, to prevent the way from being opened again for unlimited copying, a "copy" of the multimedia data stream has to be carried out device-specific for another device of a user as well. At the same time it is absolutely significant  
25 that the origin of each copy of a multimedia piece can be tracked down, i.e. it should always be possible to ascertain without doubt who has created a multimedia piece (author, composer), who has put it into circulation (provider, distributor, supplier), who has made an intermediate  
30 copy, and who has possibly made a further intermediate copy, etc. Only when the origin is known a user of a multimedia piece can prove without doubt that he uses the multimedia piece legally, or only then an illegal user can be  
35 found guilty without doubt.

5 Furthermore it is possible to carry out the binding of the  
multimedia data not to one player directly, but to bind the  
data to a "Smart Card". Thereby identical multimedia data  
streams can be maintained on various devices, but can only  
be used on the respective device where the Smart Card is  
10 inserted at that time.

Therefore, according to the present invention a second data  
stream is generated from a first data stream comprising a  
first payload data block with multimedia data, that also  
15 comprises a first header and a first payload data block  
with multimedia data, a second data stream is generated  
that also comprises again a header and a payload data  
block. However, in this second header, i.e. the header of  
the second data stream according to the present invention  
20 at least those parts of the first header, i.e. the header  
of the first data stream allowing conclusions as to the  
origin of the multimedia data are included. The second pay-  
load data block comprises the same multimedia data as the  
first payload data block, i.e. the payload data block of  
25 the first data stream.

The header of the second data stream can essentially have  
the same format as the header of the first data stream.  
However, it includes Besides the usual header information  
30 comprises additionally at least the information from the  
first header allowing conclusions as to the origin of the  
multimedia data.

Essentially, in a preferred embodiment of the present in-  
35 vention, the whole first header is entered into the second  
header. In order to protect the second header comprising  
the first header from manipulation it can additionally be

5 provided with a digital signature that is derived from the data of the second (current) header and above that from the data of the first (old) header. In a preferred embodiment of the present invention, data from the first header allowing conclusions as to the origin of the multimedia data  
10 comprise a supplier identification, i.e. an identification of the supplier of the first data stream that could for example be the Deutsche Telekom (German telecommunications company), as well as author information allowing conclusions as to the author or composer, as well as a user identification, i.e. an identification of the device for which  
15 the data stream has originally been licensed.

It is a specific advantage of the inventive concept that it can be carried out as often as desired what leads to a multiply recursive header structure since a third data stream  
20 that comprises a third header and a third payload data block again comprises origin information of the second header in its header. This origin information is on the one hand the origin information of the first header and on the other hand the origin information of the second header.  
25 Analogous to the origin information of the first header the origin information of the second header is for example an identification of the device the piece was originally licensed for by the original supplier and an identification  
30 of the device a "copy" was made for, for example an identification of a car hifi system.

Here, it will be especially noted that the author information of the first header is also present in the header of  
35 the third data stream. Thus, the inventive concept is in conformity with statutory regulations regarding any program or any apparatus removing author information as illegal.

5 Such statutory regulations have already become national law  
in the United States and it might only be a question of  
time when these regulations will be nationalized Europe  
wide.

10 In a preferred embodiment of the present invention the part  
of an old header taken over into the new header contains  
only licensing information referring to the manner how a  
licensed multimedia piece may be used, i.e. how often it  
may be played and how often it may be copied or whether a  
15 copy of a copy is legal or not.

The payload data block can of course be encrypted symmetri-  
cally, while the key of the symmetrical encrypting method  
is encrypted asymmetrically. In this case an apparatus for  
20 generating the second data stream will carry out a complete  
decryption from the first data stream and subsequently a  
complete new encryption.

Thus, the inventive concept allows full protection of a  
25 multimedia piece in a way from the author or composer via  
an arbitrary number of copies to an end user. Above that,  
the origin of a current copy can be tracked down unbrokenly  
at any time of a copy or distribution chain whereby the  
number of copies or distribution processes is arbitrary.  
30 Additionally, author information is considered any time  
whereby copyright protection is satisfied. Finally, the in-  
ventive concept can be implemented efficiently and flexible  
such that it is also suitable for inexpensive players with  
limited memory and processor resources, that it is easy to  
35 handle, and that modern client demands for high flexibility  
are fully considered.

5

Brief Description of the Drawings

- Fig. 1 shows a multimedia data stream, which can be produced according to the present invention;
- 10 Fig. 2 shows a detailed illustration of the header and the payload data block of the encrypted multimedia data stream;
- 15 Fig. 3 shows a selection of certain entries into the individual sub blocks of the header block;
- Fig. 4 a schematic illustration of a distribution scenario;
- 20 Fig. 5 a schematic view of a data stream with recursive header structure;
- Fig. 6 a flow chart of a method for generating a second data stream from a first data stream according to
- 25 the present invention; and
- Fig. 7 a method for playing a second data stream generated based on a first data stream according to
- 30 the present invention.

Detailed Description of Preferred Embodiments

- 35 Fig. 1 shows an encrypted multimedia data stream 10 comprising a header 12 and a payload data block 14 that is a block containing encrypted multimedia data. The payload

5 data block 14 includes encrypted sections 16 and unen-  
crypted sections 18 between the encrypted sections 16. In  
addition a multimedia data stream, which can be produced  
according to the present invention, includes a further un-  
encrypted section 20 following the header 12 and being ar-  
10 ranged in front of an encrypted section 16.

Usually the multimedia data to be encrypted is encoded in  
any way, such as according to a MPEG standard, such as  
MPEG-2 AAC, MPEG-4 audio or MPEG Layer-3. It is thus suffi-  
15 cient to encrypt certain sections of the multimedia data to  
be encrypted. This leads to an essentially decreased proc-  
essing expenditure both at the provider who encrypts the  
data and at the customer who in turn has to decrypt the  
data. Furthermore, the pleasure of hearing and seeing re-  
20 spectively of a user who only uses the unencrypted multime-  
dia data is seriously impaired by the constantly occurring  
encrypted blocks, when the multimedia data is only en-  
crypted partly.

25 Although Fig. 1 shows an encrypted multimedia data stream  
in which the header 12 is arranged at the beginning of the  
encrypted multimedia data stream this arrangement of the  
header and the payload data block is not to refer to the  
transmission of the encrypted multimedia data stream. The  
30 term "header" is only meant to express that a decryption  
device which is to decrypt the encrypted multimedia data  
stream at first requires at least parts of the header be-  
fore the multimedia data itself can be decrypted. Depending  
on the transmission medium the header may also be arranged  
35 at some place in the payload data block or be received af-  
ter certain parts of the payload data block when for exam-  
ple a packet-oriented transmission of the multimedia data

5 stream is thought of, in which different packets, one of  
which may contain the header and another one a part of the  
payload data block, are transmitted via different physical  
transmission ways in such a way that the order of receipt  
does not have to correspond to the order of sending. How-  
10 ever, in this case a decryption device has to be able to  
save the packets received and to order them again in such a  
way that information is extracted from the header to begin  
the decryption. The encrypted multimedia data stream may  
further be present in the form of a file or also in the  
15 form of an actual data stream, when for example a life  
transmission of a multimedia event is thought of. This ap-  
plication will especially occur with digital user-selective  
broadcasting.

20 The length of an encrypted section 16 is represented by a  
value amount 22 while the spacing in the encrypted multime-  
dia data stream from the beginning of an encrypted section  
16 to the beginning of the next encrypted section 16 is re-  
ferred to as step 24. The length of the further encrypted  
25 section 20 is given by a value first step 26.

These values 22, 24 and 26 are obviously required for a  
correct decrypting of the multimedia data in a decryption  
device. This is why they have to be entered into the header  
30 12 as will be explained later.

Fig. 2 shows a more detailed illustration of the encrypted  
multimedia data stream 10 consisting of the header 12 and  
the payload data block 14. The header 12 is divided into  
35 several sub blocks that will be explained especially refer-  
ring to Fig. 3. It is pointed out that the number and the  
function of the sub blocks can be extended at will. Thus,



5 in Fig. 2 some sub blocks of the header 12 are illustrated  
in an only exemplary way. The header includes as it is  
shown in Fig. 2 a so-called crypt-block 29 comprising, in  
general terms, relevant information for encrypting the mul-  
timedia data. In addition the header 12 includes a so-  
10 called license block 30 comprising data referring to how a  
user can or is allowed to use the encrypted multimedia data  
stream. The header 12 further includes a payload data info  
block 32 which can include information concerning the pay-  
load data block 14 and as well as general information about  
15 the header 12 itself. Furthermore the header 12 may com-  
prise an old header block 34 enabling a so-called recursive  
header structure. This block makes it possible for the user  
who, apart from a decryption device is also in the posses-  
sion of an encryption device to reformat an encrypted mul-  
20 timedia data stream for other replay instruments in his  
possession without losing or modifying the original header  
information provided by the distributor. Depending on the  
application further sub blocks, such as an IP information  
block (IP = intellectual property) according to ISO/IEC  
25 14496-1, MPEG-4, Systems, 1998, containing copyright infor-  
mation, can be added to the header 12.

As it is the standard in the art, an internal block struc-  
ture can be allocated to each block, this structure at  
30 first requesting a block identifier and including the  
length of the sub block and at last giving the block pay-  
load data itself. Thus, the encrypted multimedia data  
stream, and in particular the header of the encrypted mul-  
timedia data stream, is given an increased flexibility in  
35 such a way that it can react to new requirements in such a  
way that additional sub blocks may be added or existing sub  
blocks may be omitted.

5

Fig. 3 gives an overview of the block payload data of the individual sub blocks shown in Fig. 2.

At the beginning the crypt block 28 is explained. It contains an entry for a multimedia data encryption algorithm 10 40 identifying the symmetrical encryption algorithm used in the preferred embodiment, which has been used when encrypting the multimedia data. The entry 40 can be an index for a table in such a way that, after reading the entry 40, a decryption device is capable of selecting this encryption al- 15 gorithm the encryption device has used from a plurality of encryption algorithms. The crypt block 28 further includes the entry first step 26, the entry step 24 and the entry amount 22, which has already been illustrated in connection 20 with Fig. 1. These entries in the header enable a decryption device to subdivide an encrypted multimedia data stream accordingly to be able to carry out a correct decryption.

25 The crypt block 28 further contains an entry for the distributor or provider or supplier 42, the entry being a code for the distributor who has produced the encrypted multimedia data stream. An entry user 44 identifies the user who has obtained the encrypted multimedia data stream in some 30 way from the distributor who is identified by the entry 42. According to the invention it is preferred not to use a person-related user identification since this would open the way for illegal copies. Instead it is preferred to carry out the user identification device specific. The entry user would then for example comprise the serial number 35 of a PC, a laptop, a car hifi system, a home stereo system, smart card etc. that authorizes playing only on a certain

10

15

20

25

30

35

5 Now the license block 30 of the header 12 will be explained. The license block includes an entry bit mask 52. This entry can comprise certain specific information for replaying or for the general way of using the encrypted multimedia data. With this entry a decryption device could  
10 especially be told whether the payload data can be replayed locally or not. In addition at this point it may be signalled whether the challenge response method has been used for the encryption, this method being described in the already mentioned German patent DE 196 25 635 C1 and enabling  
15 an efficient data base access.

An entry expiration date 54 indicates the point in time at which the permission to decrypt the encrypted multimedia data stream expires. A decryption device will in this case  
20 check the entry expiration date 54 and compare it to a build-in time measuring device in order not to carry out a decryption of the encrypted multimedia data stream if the expiration date has been exceeded. This makes it possible for the provider to make encrypted multimedia data available for a limited amount of time, which has the advantage  
25 of a much more flexible handling and price setting. This flexibility is further supported by an entry starting date 56 in which it is specified from which point on an encrypted multimedia file is allowed to be decrypted. An encryption device will compare the entry starting date with  
30 its built-in watch to only carry out a decryption of the encrypted multimedia data when the current point in time is later than the starting date 56.

35 The entry allowed replay number 58 indicates how often the encrypted multimedia data stream can be decrypted, that is replayed. This further increases the flexibility of the

- 5 provider in such a way that it for example only allows a certain number of replays compared to a certain sum which is smaller than a sum which would arise for the unlimited usage of the encrypted multimedia data stream.
- 10 For verifying and supporting respectively the entry allowed replay number 58 the license block 30 further includes an entry actual replay number 60 which could be incremented by one for example after each decryption of the encrypted multimedia data stream. A decryption device will thus always
- 15 check whether the entry actual replay number is smaller than the entry allowed replay number. If this is the case, a decryption of the multimedia data is carried out. If this is not the case, a decryption is no longer carried out.
- 20 Analog to the entries 58 and 60 entries allowed copy numbers 62 and actual copy number 64 are implemented. By means of the two entries 62 and 64 it is made sure that a user of the multimedia data only copies them as often as he or she is allowed to do so by the provider or as often as he or
- 25 she has paid for when purchasing the multimedia data. By the entries 58 to 64 a more effective copyright protection is assured, a selection between private users and industrial users being attainable for example by setting the entries allowed replay number 58 and allowed copy numbers 62
- 30 to a smaller value.

The licensing could for example be designed in such a way that a certain number of copies (entry 62) of the original are allowed while copies of a copy are not allowed. The

35 header of a copy would then, unlike the header of the original, have zero as the entry allowed copy number in

5 such a way that a proper encryption/decryption device can  
no longer copy this copy.

In the example for a multimedia data protection protocol  
(MMP) shown here the header 12 further contains a payload  
10 data information block 32 having in this case only two  
block payload data entries 66 and 68, the entry 66 contain-  
ing a hash sum on the total header, while the entry 68  
identifies the type of hash algorithm having been used for  
forming the hash sum on the total header.

15 Hash algorithms are known in the art and can be used to  
form a digital signature of a data amount such that also a  
small change of data in a data amount leads to a change of  
the digital signature whereby the authenticity of data and  
20 especially of the (non encrypted) header can be checked in  
an easy and efficient way.

A preferred method for generating a digital signature is to  
form a hash sum on the whole header and to encrypt or de-  
25 crypt it asymmetrically in order to obtain the entry 66.  
Specifically, the supplier would decrypt the hash sum of  
the whole header with his private key. However, the encryp-  
tion apparatus at the customer would form the hash sum on  
the whole (eventually illegally modified) header itself and  
30 above that decrypt the entry 66 with the public key of the  
asymmetrical encryption method and then compare the two re-  
sults. If they match, the playing process will be started.  
If they don't match, no decrypting/decoding/playing is pos-  
sible.

35 In this context reference is made for example to "Applied  
Cryptography", Second Edition, John Wiley & Sons, Inc. by

5 Bruce Schneider (ISBN 0 417-11709-9) including a detailed illustration of symmetrical encryption algorithms, asymmetrical encryption algorithms and hash algorithms.

10 The header 12 finally includes the old header block 34, which, along with the synchronizing information, which is not shown in Fig. 3, comprises the entry old header 70. In the entry old header 70 the old header can be maintained by the provider if a user performs an encryption himself and thus produces a new header 12, in order not to lose essential information the provider has entered into the header.  
15 For this purpose author information (IP information block) could for example count prior user information and distributor information which enables tracing back of a multimedia file which for example has been decrypted and encrypted several times by different instruments to the  
20 original provider transparently, the author information being maintained. It is thus possible to check at any point whether an encrypted multimedia file has been acquired legally or illegally.

25

Fig. 4 shows a schematic block diagram of a scenario wherein the inventive concept can be applied in an advantageous way. An author or composer 100 has created a multimedia piece, for example a text, a piece of music, a film or  
30 a picture. He delivers this work, in this invention generally referred to as multimedia piece, to a supplier 102 of multimedia data. It is especially pointed out here that the expression "multimedia data" in the sense of the present invention comprises audio data, video data or a combination  
35 of audio and video data.

5 The supplier ensures that the multimedia piece of the  
author/composer 100 is put in circulation by encoding it  
for example according to the method MPEG layer 3 (MP3). In  
order to achieve a customer selective providing for use of  
the encoded multimedia piece the supplier 102 will bring  
10 the encoded multimedia piece into a first data stream com-  
prising a header and payload data block. A data stream as  
it might be used is illustrated in Fig. 3.

In this connection it should be especially pointed to the  
15 IP information block 72 comprising author information 74 as  
payload data identifying the author/composer or in general  
artist. The IP information block could for example be car-  
ried out according to ISO/IEC 14496-1 MPEG-4 systems, 1998.  
It could especially comprise the name of the  
20 author/composer/artist or also the ISBN number (ISBN = in-  
ternational standard book number), the ISRC code (ISRC =  
international standard recording code), the ISAN number  
(ISAN = international standard audiovisual number), the  
ISMN number (ISMN = international standard music number),  
25 etc. Such meta information will allow a unique identifica-  
tion of the author of the multimedia piece such that by  
adding these meta information to the payload data the en-  
forcement of copyrights will be much easier.

30 The supplier of multimedia data 102 generates a first data  
stream comprising a first header and a first payload data  
block. All the data illustrated in Fig. 3 can be included  
in the header, wherein the author information (entry 74),  
the distributor identification (entry 42) and the user  
35 identification (entry 44) should be especially noted. While  
the author information (entry 74) represents the origin of  
the multimedia piece in general, the distributor identifi-



5 cation (42) uniquely defines the origin of the first data  
stream while the user identification defines the "destina-  
tion" of the first data stream, i.e. the device that is al-  
lowed to use the data stream and that has also paid for it,  
whereby on the one hand the service of the supplier 102 of  
10 multimedia data is paid and on the other hand royalties to  
the author/composer 100 can flow. In the first header of  
the first data stream a receiver-PC 104 could for example  
be identified by the user identification 44. The first data  
stream can now on the one hand be played on the receiver-PC  
15 104, however, according to the invention, the receiver-PC  
is defined in such a way that it can also generate a "copy"  
of the first data stream in order to generate one or several  
second data streams comprising in their header the user  
identification 44 of a car hifi system 106a, a home hifi  
20 system 106b, a solid state player 106c, etc.

Every second header will essentially comprise the same pay-  
load data block, the header of every second data stream,  
i.e. the second header, will however be different regarding  
25 the user identification 44. However, according to the in-  
vention, every second header will comprise information al-  
lowing conclusions as to the origin of the respective sec-  
ond data stream. This information can comprise author in-  
formation, an identification for the receiver-PC 104 and an  
30 identification for the supplier 102 of the first data  
stream. Preferably, the second header additionally com-  
prises licence information referring to the fact how often  
the multimedia piece may be played or how often it may be  
copied. It can especially happen that for example five cop-  
35 ies are allowed but no copy of the copy is allowed. In the  
entry allowed copy number 62 of the first header there  
would for example be five. In the entry allowed copy number

5 of the second header however, there would be zero. Even  
when the car hifi system 106a, the home hifi system 106b or  
the solid state player 106c were designed in such a way  
that it can carry out a decryption or an encryption by it-  
self, i.e. like the receiver-PC 104, still no further copy  
10 would be produced, i.e. no third data stream, since the en-  
try 62 in the second header of the second data stream is  
set to zero. If this were not the case and if the copy of a  
copy were allowed the devices 106a to 106c could again cre-  
ate third data streams but would comprise origin informa-  
15 tion of the respective second data stream and naturally of  
the respective first data stream.

This results in a recursive header structure shown sche-  
matically in Fig. 5 that can principally be repeated arbi-  
20 trarily. Fig. 5 shows an nth data stream 110 comprising an  
nth header 112 and an nth payload data block 114. The nth  
header 112 again comprises a (n-1)th header that again com-  
prises a (n-2)th header, etc.

25 Preferably, the supplier of multimedia data 102 (Fig. 4)  
encrypts the multimedia data in the first payload data  
block at least in parts. Preferably, a symmetrical encrypt-  
ing method for encrypting the multimedia data is used,  
wherein the key of the symmetrical encrypting method is  
30 again encrypted asymmetrically. The asymmetric key en-  
crypts with the private key of the supplier 102 for the  
symmetrical encrypting method is the output value 46 (Fig.  
3). The receiver-PC 104 will therefore need the respective  
public key of the supplier 102 of multimedia data in order  
35 to decrypt the output value 46 again, in order to obtain  
the key for the symmetrical decrypting method that the sup-  
plier 102 of multimedia data has used as well. The re-

5     ceiver-PC 104 is now enabled to play the first data stream.  
If the first data stream is encoded the receiver-PC 104  
carries out a decoding prior to playing. The sequence will  
therefore be: decrypting, decoding, and playing.

10    However, the receiver-PC should also be able to generate a  
second data stream for a specific additional player 106a to  
106c. In this case the receiver-PC 104 can be configured  
for encrypting the multimedia data that are decrypted,  
wherein a symmetrical encrypting method is preferred due to  
15    speed aspects. The receiver-PC 104 will again asymmetri-  
cally encrypt the key for the symmetrical encrypting method  
with its private key, provide the second header with its  
own identification as distributor entry 42 and further pro-  
vide the second header with the identification for example  
20    of the car hifi system as user identification 44. Further,  
the receiver-PC 104, will generate a different output value  
that will be entered into the entry 46 of the second header  
since the receiver-PC has a different data key than the  
supplier 102 of multimedia data. Above that, the receiver-  
25    PC will update the licence-block of the second header as  
desired. However, according to the invention, it will pref-  
erably write the whole first header into the entry old  
header 70 in such a way that all information of the first  
header are maintained and especially the origin information  
30    of the first data stream as it has been described several  
times.

Neither the first, second or the nth header are encrypted  
themselves. In order to protect the respective headers from  
35    attacks after the completion e.g. of the second header a  
hash sum is formed on the header for example according to a  
hash algorithm identified in entry 68 (Fig. 3). Preferably,

5 this hash sum is not only formed by the blocks 28, 30, 32,  
72 of the second header but it also comprises the block for  
the old header 34. This hash sum can then be directly en-  
tered into the entry 66 (Fig. 3). For the increase of  
safety it is however preferred to enter a digital signature  
10 for the hash sum of the second header. A digital signature  
of the hash sum on the second header could for example be  
again formed with an asymmetrical encryption method in such  
a way that the receiver-PC 104 generating the second data  
stream encrypts the hash sum on the second header with its  
15 own private key and writes the result into the entry 66.

The home hifi system 106b will now at first verify the sec-  
ond data stream by also forming a hash sum on the second  
header as it is supplied to the home hifi system. Further,  
20 the home hifi system 106b will decrypt the entry 66 in the  
second header with the public key of the receiver-PC 104  
and compare the obtained result with the just calculated  
hash sum. If both hash sums are the same it can be assumed  
that the second data stream has not been manipulated. If  
25 the two results differ, a legally implemented car hifi sys-  
tem will not continue playing since it can be assumed that  
unallowed manipulations have been carried out either at the  
second header or in a way "belated" at the first header.

30 Fig. 6 shows a flow chart for the inventive method for gen-  
erating a second data stream from a first data stream that  
is carried out by the receiver-PC 104 in order to "retag"  
the device specifically licensed first data stream to other  
devices (106a to 106c).

35

Basically, the receiver-PC 104 will at first extract the  
header from the first data stream (116). Above that, the

5 receiver-PC 104 will generate a second header for the second data stream (118) as far as possible. This header generated as far as possible could comprise all information of the header shown in fig. 3 (blocks 28, 30, 32, 34, 72), but not the old header block 34. This block will be described  
 10 in a step 120, wherein at least the origin information from the first header is entered into the entry 70. However, for safety reasons and also for implementation reasons it is preferred to enter not only the origin information from the first header but also all information from the first header  
 15 into the entry 70 of the second header. This could lead to the fact that certain information exist twice, like e.g. the author information 74 as well as information from other blocks, for example first step 26, step 24, amount 22, etc. Already here it can be seen that by the fact that the re-  
 20 ceiver-PC 104 generates a complete second header in step 118 it is not bound to the parameters of the supplier 102 of multimedia data. For example, a less expensive encrypting method could be applied in order to enable the second data stream to be encrypted with less effort again for ex-  
 25 ample by the solid state player 106c that needs, as known, limited memory and processor resources in order to be offered inexpensively. Considering these aspects the payload data block of the second data stream might even not be encrypted anymore at all, if preferred.

30

Finally, the receiver-PC 104 generates a second payload data block for the second data stream (122) in order to finally obtain the second data stream.

35 The flow chart in Fig. 7 describes in general a method for playing a second data stream generated based on a first data stream, wherein this method could be carried out in

5 one of the devices 106a to 106c. If between the supplier  
102 of multimedia data and the receiver-PC 104 a further  
intermediate distributor as for example a "retailer" of  
multimedia data is disposed whom the supplier 102 of multi-  
media data who will then have a wholesaler function sup-  
10 plies, the inventive method generally illustrated in Fig. 7  
would already be carried out by the receiver-PC 104.

Generally, the method for playing can be started with the  
step of reading the second header of the second data stream  
15 (130). The device 106a will then for example extract the  
part of the first header comprising origin information,  
i.e. the old header block 34 and read the payload data of  
the entry 70 (132).

20 In order to prevent the playing of illegal pieces the ori-  
gin of the second data stream is verified in step 134 using  
the origin information in entry 70. Such a verification  
could for example consist of checking whether origin infor-  
mation is present in the second header at all (136). If it  
25 is found out in the verification 136 that no origin infor-  
mation is present in the second header at all, a legally  
driven playing apparatus according to the present invention  
will refuse playing and will stop the operation (138). If  
it is found out in this simple form of verification 136  
30 that origin information is present and that it makes sense  
and is no "deception data" of some sort, the inventive  
playing apparatus will begin or continue playing the second  
data stream (140).

35 A more expensive way of verification could be to test  
whether the supplier identification 42 of the second header  
matches the user identification 44 of the first header. In

5 this case it would be proved without doubt that the copy present in the player comes from the respective home-PC. Any further verification techniques with more or less effort are considered.

10 In a preferred embodiment of the present invention it is preferred to carry out the verification via a digital signature comprising both data of the first header and data of the second header, as it has been described in connection with Fig. 4. Further even more complicated methods can also  
15 be used for verification wherein however always the origin of the present data stream is tested that can either be author information or other respective supplier entries 42 or user entries 44 of the individually embedded header of the generally spoken multiply recursive header structure  
20 that is illustrated in Fig. 5.

Besides the verification of the origin of the second data stream (step 134 in Fig. 7) the player will preferable be implemented in such a way that it processes also the licence block 30 and especially for example according to the  
25 entries 58 and 60 processes regarding to the authorized or actual playing number in order to find out whether it may play a data stream. The player will of course use the other information of the second header in the described manner if  
30 the second data stream is encrypted in order to finally decrypt, decode and play the second data stream.

5

Claims

1. Method for generating a second data stream from a first data stream which comprises a first header (12) and a first payload data block (14) with payload data, the method comprising the following steps:

10 extracting (116) the first header (12) from the first data stream;

15 generating (118) a second header for the second data stream;

20 entering (120) at least a part (42, 44, 74) of the first header into the second header, the part of the first header including information which allows conclusions as to the origin of the payload data; and

25 generating (122) a second payload data block having the same payload data as the payload data block of the first data stream, so as to obtain the second data stream.

30 2. Method as claimed in claim 1, wherein the information allowing conclusions as to the origin of the first data stream includes an identification (42) for a supplier of the first data stream.

35 3. Method as claimed in claim 1 or 2, wherein the information allowing conclusions as to the origin of the first data stream includes author information (74), such as the author, the component, the ISRC number, the ISAN number or the ISMN number of the payload data of the first data stream.

40 4. Method as claimed in ~~any of the preceding claims~~ claim 1, wherein the part of the first header, which is entered into the second header, further comprises an



5 identification ~~(44)~~ of the receiver of the first data stream.

10 5. Method as claimed in claim 4, wherein the identification is device-specific, and the receiver ~~(104)~~ of the first data stream is a player indicated by the identification, or a smart card.

15 6. Method as claimed in ~~any of the preceding claims~~ claim 1, wherein the part of the first header which is entered into the second header further comprises licence data ~~(30)~~ relating to the manner in which a receiver ~~(104)~~ of the first data stream may use the same, the licence data of the first header specifying the licence data of the second header.

20 7. Method as claimed in claim 6, wherein the licence data ~~(30)~~ of the first header specify that the first data stream may be copied a certain number of times ~~(62)~~, that no copy may be taken of a copy, however, the step of generating ~~(118)~~ the second header for the second data stream including the entering of second licence information into the second header of the second data stream, such that no more copy may be taken of the second data stream.

30 8. Method as claimed in ~~any of claims 4 to 7~~ claim 4,

35 wherein the step of generating ~~(118)~~ a second header comprises the step of entering an identification ~~(44)~~ for the receiver ~~(106a to 106c)~~ of the second data stream as a user identification, and of entering an identification of the receiver ~~(104)~~ of the first data stream as a supplier identification ~~(42)~~, and

40 wherein the step of entering ~~(120)~~ at least a part of the first header into the second header comprises the entering of the identification of the supplier ~~(42)~~

5 of the first data stream as a supplier identification, and the entering of the identification ~~(44)~~ of the receiver of the first data stream as a user identification into a part of the second header, which is reserved for information of the first header.

10

9. Method as claimed in ~~any of the preceding claims~~ claim 1, which further comprises the following step:

15

issuing a digital signature ~~(66)~~ for the second header, including the part of the first header, and attaching the digital signature to the second header.

10. Method as claimed in claim 9, wherein the issuing step further comprises the following substeps:

20

forming a hash sum over the second header, including the part ~~(34)~~ of the first header, using a specified hash algorithm ~~(68)~~; and

25

encrypting the hash sum by means of an asymmetric encrypting method using a private key of the receiver ~~(104)~~ of the first data stream.

30

11. Method as claimed in ~~any of the preceding claims~~ claim 1, wherein the payload data in the payload data block ~~(14)~~ are at least partly encrypted and wherein encrypting information is contained in the first header, the step of generating ~~(118)~~ the second header further comprising the following steps:

35

decrypting the first payload data block of the first data stream using the encrypting information ~~(46, 40, 22 to 26)~~ in the first header;

40

encrypting the decrypted payload data and entering corresponding encrypting information ~~(46, 40, 22 to 26)~~ into the second header,

5

the encrypting information of the first header also being entered into the second header.

10

12. Method as claimed in claim 11, wherein the encrypted payload data in the first payload data block ~~(14)~~ are encrypted symmetrically and wherein the key is again encrypted asymmetrically using a private key, the decrypting step comprising the following steps:

15

decrypting the encrypted key ~~(46)~~ by means of the public key of the supplier ~~(102)~~ so as to obtain the key for a symmetric decryption ~~(40)~~;

20

encrypting a payload data key of the decrypted payload data using a private key of a receiver ~~(104)~~ of the first data stream carrying out the method for generating a second data stream; and

25

entering the asymmetrically encrypted payload data key into the second header ~~(46)~~.

30

13. Method as claimed in ~~any of the preceding claims~~ claim 1, wherein in the step of entering ~~(120)~~, the entire first header is entered into the second header.

35

14. Method as claimed in ~~any of the preceding claims~~ claim 1, wherein the first header itself comprises at least a part of a header of a data stream which relates to the origin of the first data stream, such that the entering step results in a multiply recursive header structure ~~(Fig. 5)~~.

40

15. Method for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, wherein at least a part ~~(70)~~ of the first

5 header which comprises information regarding the origin of the first data stream, is contained in the second header, the method comprising the following steps:

10 extracting ~~(132)~~ the part ~~(70)~~ of the first header from the second header;

15 verifying ~~(134)~~ the origin of the second data stream using the part ~~(70)~~ of the first header which comprises information regarding the origin of the first data stream; and

in case of a positive result of the verifying step ~~(136)~~, playing ~~(140)~~ the second data stream.

20 16. Method as claimed in claim 15, wherein the second header of the second data stream has a digital signature ~~(66)~~ attached to it which fits the part ~~(70)~~ of the first header, and wherein the verifying step comprises the following substep:

25 checking the authenticity of the second header using the digital signature ~~(66)~~.

30 17. Method as claimed in claim 16, wherein the digital signature ~~(66)~~ is the result of an encryption of a hash sum of the second header, which encryption has been carried out by means of a private key of the apparatus ~~(104)~~ having generated the second data stream, the step of checking the authenticity comprising the following steps:

40 decrypting the digital signature by a public key of the apparatus ~~(104)~~ which has generated the second data stream, so as to obtain the hash sum of the second header;

forming a hash sum of the present header;

5

comparing the hash sums;

in case of the hash sums matching, issuing a positive verification result—(136).

10

18. Method as claimed in claim 17, wherein the part (70) of the first header further comprises licence information (30)—regarding the manner in which the first data stream may be utilized, and wherein the second header comprises licence data (30)—derived from the licence data of the first header, the method further comprising the following substeps:

15

20

comparing the licence data of the second header and the first header so as to evaluate the authenticity of the licence data of the second header;

in case of questionable authenticity, blocking (138) the playing of the second data stream.

25

19. Apparatus (104)—for generating a second data stream from a first data stream which comprises a first header (12)—and a first payload data block (14)—with payload data, the apparatus comprising the following:

30

means for extracting (116)—the first header (12)—from the first data stream;

35

means for generating (118)—a second header for the second data stream;

40

means for entering (120)—at least a part (42, 44, 74) of the first header into the second header, the part of the first header including information which allow conclusions as to the origin of the payload data; and

- 5 means for generating ~~(122)~~ a second payload data block which comprises the same payload data as the payload data block of the first data stream, so as to obtain the second data stream.
- 10 20. Apparatus ~~(104)~~ as claimed in claim 19, which is designed as a personal computer.
- 15 21. Apparatus ~~(106a to 106e)~~ for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, at least a part ~~(70)~~ of the first header, which comprises information regarding the origin of the first data stream, being contained in the second header, the apparatus comprising the following:
- 20 means for extracting ~~(132)~~ the part ~~(70)~~ of the first header from the second header;
- 25 means for verifying ~~(134)~~ the origin of the second data stream using the part ~~(70)~~ of the first header which comprises information regarding the origin of the first data stream; and
- 30 means for playing the second data stream, which responds to the means for verifying ~~(134)~~, so as to play the second data stream only if the means for verifying ~~(134)~~ provide a positive result.
- 35 22. Apparatus as claimed in claim 21, which is designed as a hifi system ~~(106b)~~, as a car hifi system ~~(106a)~~, as a portable multimedia player ~~(106e)~~, as a computer or as a component of any of the above-mentioned devices.
- 40

5       **Method and Apparatus for Generating a Data Stream and**  
          **Method and Apparatus for Playing a Data Stream**

Abstract

10

      In a method for generating a second data stream from a  
      first data stream, which comprises a first header and a  
      first payload data block with payload data, the first  
      header is initially extracted ~~(116)~~ from the first data  
15   stream. Subsequently the second header for the second data  
      stream is generated ~~(118)~~. Then, at least a part of the  
      first header is entered ~~(120)~~ into the second header, the  
      part of the first header including information, which al-  
      lows conclusions as to the origin of the payload data. Fi-  
20   nally, the second payload data block is generated ~~(122)~~,  
      which comprises the same payload data, so as to obtain the  
      complete second data stream. The method according to the  
      invention enables device-specific encrypting of payload  
      data, a flexible, device-specific "copy" for other devices  
25   of a user and, in particular, complete documentation of the  
      origin of the present copy, such that effective copyright  
      protection may be realized.